

Il futuro del modello Zero Trust

Questo articolo rappresenta l'ultimo contenuto della nostra serie di approfondimenti sull'architettura Zero Trust. In questo approfondimento finale, analizziamo l'implementazione pratica del modello Zero Trust attraverso l'integrazione sinergica di scelte organizzative e tecnologiche.

L'adozione di un modello Zero Trust richiede un'integrazione sinergica di scelte organizzative e tecnologiche, finalizzate sia all'implementazione del modello, sia all'incremento del valore aggiunto fornito agli utenti all'interno del perimetro di sicurezza. L'approccio Zero Trust non è un progetto con un termine predefinito, ma un processo in continua evoluzione che richiede un impegno costante per essere mantenuto e migliorato nel tempo.

Come discusso, è necessario:

- Identificare in modo robusto gli utenti. L'organizzazione deve promuovere l'adozione di tecnologie di autenticazione multifattore. Tecnologie come l'autenticazione senza password (passwordless) e il single sign-on possono semplificare l'esperienza di accesso degli utenti, garantendo al contempo un elevato livello di sicurezza. Inoltre, l'adozione di strumenti di autenticazione basati su biometria o su fattori contestuali (come la posizione o il dispositivo utilizzato) può ulteriormente rafforzare la robustezza del processo di identificazione.
- Identificare e gestire i dispositivi aziendali. Solo i dispositivi gestiti e autorizzati dovrebbero essere in grado di accedere ai servizi, garantendo così l'integrità, la riservatezza e la disponibilità dei dati aziendali. Tecnologie che consentono agli utenti di

installare applicazioni da un paniere pre-approvato, o policy di compliance che li rendono amministratori dei propri dispositivi, possono incrementare l'autonomia senza compromettere la sicurezza. Inoltre, l'adozione di soluzioni di Mobile Device Management (MDM) e di Endpoint Detection and Response (EDR) consente un monitoraggio costante dello stato dei dispositivi, garantendo che questi siano sempre conformi alle politiche di sicurezza aziendali.

- Identificare e gestire le reti e il perimetro di accesso. Non è sufficiente trovarsi in un determinato luogo o essere connessi alla rete aziendale per ottenere accesso ai sistemi e ai dati aziendali. Tecnologie di Network Access Control (NAC) che regolano dinamicamente il livello di fiducia possono mitigare l'impatto di una eventuale compromissione del dispositivo dell'utente. L'adozione di segmentazione della rete, sia fisica che logica, permette di limitare la propagazione di eventuali attacchi, mentre l'uso di micro-segmentazione offre un ulteriore livello di protezione limitando l'accesso alle risorse su base granulare.
- Gestire gli applicativi e gli accessi. Una lista di applicazioni consentite e vietate tutela sia l'organizzazione che gli utenti, aumentando al contempo l'autonomia operativa all'interno di un perimetro definito. I privilegi minimi di accesso rappresentano una doppia garanzia per l'utente e per l'organizzazione. Inoltre, la definizione di criteri di accesso basati sul principio del "bisogno di sapere" (need-to-know) e del "privilegio minimo" (least privilege) consente di ridurre ulteriormente il rischio di accesso non autorizzato a informazioni sensibili.
- Monitorare e aggiornare il modello organizzativo. Il team di sicurezza deve eseguire monitoraggi regolari delle metriche di controllo e suggerire miglioramenti continui al modello organizzativo e alle tecnologie adottate per ridurre il rischio cyber. L'adozione di un

approccio basato sull'analisi del rischio consente di identificare e prioritizzare le aree di intervento, mentre l'utilizzo di tecniche di threat intelligence permette di adattare il modello alle minacce emergenti, migliorando la capacità di prevenzione e risposta.

L'adozione di tecnologie appropriate, insieme alla definizione e all'implementazione di un modello organizzativo di sicurezza, conduce alla minimizzazione del rischio cyber e a una maggiore consapevolezza della sua riduzione continua. Le sole tecnologie non sono sufficienti; un modello organizzativo senza supporto tecnologico potrebbe risultare eccessivamente rigido, compromettendo l'operatività e, di conseguenza, la qualità dei servizi e del business.

Allo stesso modo, un approccio esclusivamente tecnologico, senza una struttura organizzativa adeguata, rischia di non essere sufficientemente resiliente o di non essere accettato dagli utenti, compromettendo l'efficacia complessiva delle misure di sicurezza adottate. L'equilibrio tra tecnologia e organizzazione è quindi essenziale per raggiungere una postura di sicurezza matura e sostenibile.

Implementazione ed Evoluzione del Modello Zero Trust

L'esperienza maturata negli ultimi anni nell'implementazione di architetture Zero Trust ha rivelato che il successo di questa trasformazione va ben oltre l'aspetto puramente tecnologico. Le organizzazioni che hanno ottenuto i risultati migliori hanno compreso che si tratta di un profondo cambiamento culturale e organizzativo. Il MIT Sloan Center for Information Systems Research ha documentato come le implementazioni di maggior successo abbiano dedicato una parte sostanziale delle risorse, circa il 30%, alla gestione del cambiamento culturale e alla formazione del personale.

Questo cambiamento culturale si manifesta attraverso una nuova consapevolezza della sicurezza che permea tutti i livelli dell'organizzazione. Non si tratta più di vedere la sicurezza come un ostacolo o un semplice requisito di compliance, ma come un elemento abilitante per l'innovazione e la crescita aziendale, al pari dei processi di qualità che ormai si sono consolidati nelle aziende in cui il miglioramento continuo è base per una crescita costante.

Le organizzazioni stanno sviluppando programmi di formazione continua che non si limitano a insegnare le procedure di sicurezza, ma che aiutano i dipendenti a comprendere il loro ruolo attivo nella protezione degli asset aziendali, al pari di come coinvolgono gli stessi dipendenti nell'ambito dei processi informativi/formativi della sicurezza negli ambienti di lavoro, ma mentre per questi ultimi i processi sono formalizzati a livello normativo, ancora oggi per la sicurezza informatica la definizione delle azioni è lasciata alle aziende ed altri enti.

L'implementazione di Zero Trust si è dimostrata tanto più efficace se messa in atto seguendo un percorso graduale e ben pianificato. Le esperienze sul campo mostrano che la trasformazione richiede tipicamente diversi anni per raggiungere la piena maturità. Il processo inizia con la costruzione di solide fondamenta nei primi 6-12 mesi, durante i quali l'organizzazione si concentra sulla gestione delle identità e degli accessi, introducendo l'autenticazione multi-fattore e realizzando un accurato inventario degli asset. Questa fase iniziale è cruciale per costruire la fiducia degli utenti nel nuovo modello e per identificare eventuali criticità da affrontare.

La fase successiva, che tipicamente si estende per 12-24 mesi, vede l'organizzazione espandere il modello a sistemi sempre più critici. È in questo periodo che si implementano tecnologie più sofisticate come la micro-segmentazione della rete e si inizia ad automatizzare le policy di compliance.

L'esperienza mostra che questa fase richiede un delicato equilibrio tra sicurezza e usabilità: le organizzazioni più lungimiranti hanno compreso l'importanza di coinvolgere gli utenti finali nel processo di design delle soluzioni, per garantire che le misure di sicurezza non ostacolino la produttività.

I risultati di questa trasformazione sono stati documentati in dettaglio da Forrester Research, che ha evidenziato benefici tangibili non solo in termini di sicurezza, con una riduzione del 50% delle violazioni, ma anche in termini di efficienza operativa, con una diminuzione del 30% nei costi di gestione della sicurezza. Particolarmente interessante è il miglioramento della produttività degli utenti, che hanno beneficiato di processi di accesso più snelli e intuitivi.

Guardando al futuro, il modello Zero Trust dovrà evolversi per affrontare nuove sfide tecnologiche. L'espansione dell'edge computing e dell'Internet of Things sta già ponendo nuove domande su come applicare i principi Zero Trust in contesti con risorse computazionali limitate e requisiti di latenza stringenti. L'avvento del quantum computing richiederà un ripensamento fondamentale dei meccanismi di crittografia e autenticazione, mentre l'intelligenza artificiale offrirà nuove opportunità per rendere le decisioni di sicurezza più contestuali e adattive.

Il panorama normativo in continua evoluzione rappresenta un'altra sfida significativa. Le organizzazioni dovranno bilanciare le esigenze di sicurezza con requisiti sempre più stringenti in termini di privacy e protezione dei dati personali. Questo richiederà una maggiore granularità nel controllo degli accessi e una completa tracciabilità delle decisioni di sicurezza.

Per navigare con successo questa trasformazione, le organizzazioni devono adottare un approccio equilibrato che consideri tecnologia, processi e persone come elementi

ugualmente importanti. La formazione continua deve diventare parte integrante della cultura aziendale, mentre le metriche di successo devono essere chiare e misurabili. La flessibilità dell'architettura è fondamentale per adattarsi a nuove tecnologie e minacce, così come la collaborazione attiva con partner e fornitori per estendere il modello Zero Trust all'intera catena del valore.

In conclusione, il futuro della sicurezza informatica sarà inevitabilmente basato su modelli Zero Trust, ma il successo della loro implementazione dipenderà dalla capacità delle organizzazioni di creare un ecosistema di sicurezza resiliente e adattivo. La vera sfida non sarà tanto tecnologica quanto culturale: le organizzazioni che riusciranno a integrare la sicurezza nel loro DNA, rendendola parte naturale dei processi decisionali e operativi, saranno quelle che trarranno i maggiori benefici da questa trasformazione.

Per approfondire ulteriormente questi concetti e scoprire le strategie pratiche per una corretta implementazione del modello Zero Trust, vi invitiamo a scaricare il white paper "Zero Trust: solo un problema tecnologico?" redatto dal Dott. Ing. Fabrizio Fioravanti.

Profilo Autore



Fabrizio Fioravanti è attualmente responsabile dell'Unità di Processo Sistemi, tecnologie cloud e di sicurezza informatica presso l'Università degli Studi di Firenze.

Laureato in Ingegneria Elettronica, ha successivamente conseguito il dottorato di ricerca in Ingegneria Informatica e delle Telecomunicazioni e da oltre 25 anni lavora nel settore ICT.

Ha diverse pubblicazioni scientifiche al suo attivo sia su riviste italiane che internazionali, sia che in conferenze, oltre a monografie complete o contributi a monografie.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/zero-trust-modello/>